

**(19) World Intellectual Property Organization  
International Bureau**



**(43) International Publication Date**  
**23 October 2003 (23.10.2003)**

PCT

(10) International Publication Number  
**WO 03/088566 A1**

**(51) International Patent Classification<sup>7</sup>:** **H04L 9/32**

**(21) International Application Number:** PCT/SE02/00588

(22) International Filing Date: 9 April 2002 (09.04.2002)

(25) **Filing Language:** English

(26) **Publication Language:** English

(71) Applicant (for all designated States except US): TELEFONAKTIEBOLAGET L M ERICSSON (PUBL) [SE/SE]; S-126 25 Stockholm (SE).

**(72) Inventor:** and

(75) **Inventor/Applicant (for US only):** AXELSSON, Stefan  
[SE/SE]; Ljungkullen 66, S-433 66 Sävödalén (SE).

(74) Agent: ERICSSON AB; Patent Unit West, S-431 84 Mölndal (SE).

(81) **Designated States (national):** AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MY, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

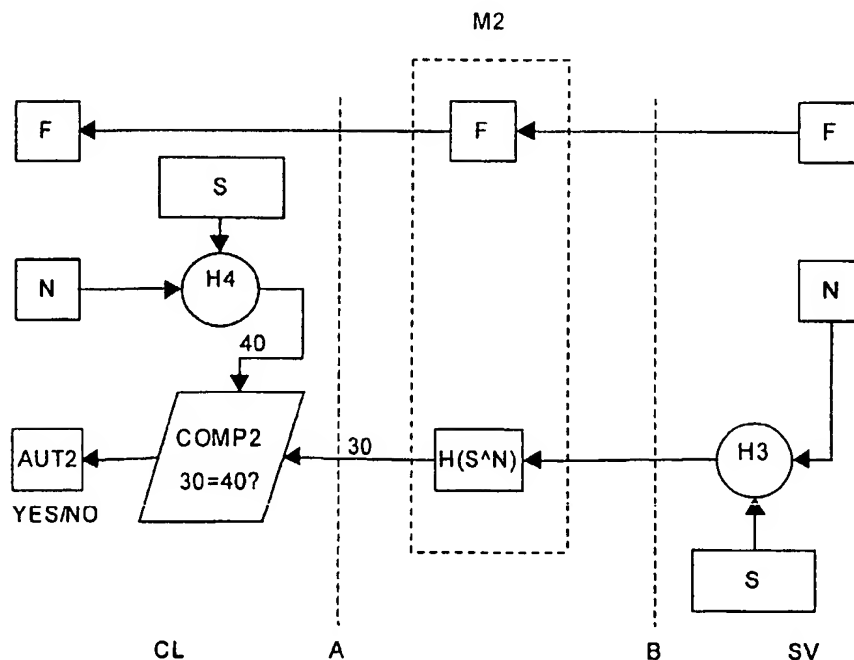
**(84) Designated States (regional):** ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Published:**

— with international search report

*For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: SECURE FILE TRANSFER



**(57) Abstract:** A method and apparatus are provided for identification/authentication of file transfers, that limits the attackers window of opportunity and that aims at incurring a minimum of overhead on the information processing between a client (CL) and a server (SV). According to a preferred embodiment of the invention hash functions (H1-H4) are involved at the server side and the client side. The client and server share a common secret value (S).

**WO 03/088566 A1**